



***Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy***



070.206 CHFS Remote User Support


**Version 2.1
January 27, 2017**

070.206 CHFS Remote User Support	Current Version: 2.1
070.000 Administrative	Review Date: 01/27/2017

Revision History

Date	Version	Description	Author
9/1/2002	1.0	Effective Date	CHFS OATS Policy Charter Team
1/27/2017	2.1	Revision Date	CHFS OATS Policy Charter Team
1/27/2017	2.1	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS Chief Information Officer (or designee)	1/27/2017	Robert Puff	

070.206 CHFS Remote User Support	Current Version: 2.1
070.000 Administrative	Review Date: 01/27/2017

Table of Contents

1	070.206 CHFS REMOTE USER SUPPORT	4
1.1	PURPOSE	4
1.2	SCOPE	4
1.3	ROLES AND RESPONSIBILITIES	4
1.3.1	<i>OATS Information Security Team.....</i>	<i>4</i>
1.3.2	<i>Privacy Lead.....</i>	<i>4</i>
1.3.3	<i>CHFS Staff and Contract Employees.....</i>	<i>4</i>
1.4	MANAGEMENT COMMITMENT.....	5
1.5	COORDINATION AMONG ORGANIZATIONAL ENTITIES	5
1.6	COMPLIANCE	5
2	POLICY REQUIREMENTS	5
2.1	GENERAL	5
3	POLICY MAINTENANCE RESPONSIBILITY	6
4	EXCEPTIONS.....	6
5	POLICY REVIEW CYCLE.....	6
6	REFERENCES.....	6

070.206 CHFS Remote User Support	Current Version: 2.1
070.000 Administrative	Review Date: 01/27/2017

1 070.206 CHFS Remote User Support

Category: 070.000 Administration

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to manage a CHFS Remote User Support Policy. This document establishes the agency's CHFS Remote User Support Policy, which reduces the overall risk(s), and provides guidelines for security best practices regarding remote user support.

1.2 Scope

The scope of this policy applies to all CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer, application, and data communication systems.

1.3 Roles and Responsibilities

1.3.1 OATS Information Security Team

Responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This team is responsible for the adherence of the CHFS Remote User Support Policy.

1.3.2 Privacy Lead

The individual(s) responsible for providing security and privacy guidance for protection of Personally Identifiable Information (PII), Electronic Protected Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role is responsible for the adherence of the CHFS Remote User Support Policy in concert with the OATS Information Security (IS) Team.

1.3.3 CHFS Staff and Contract Employees

Individual(s) must adhere to the CHFS Remote User Support Policy as well as referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system.

070.206 CHFS Remote User Support	Current Version: 2.1
070.000 Administrative	Review Date: 01/27/2017

1.4 Management Commitment

OATS Division Directors and the OATS Chief Information Officer (CIO) approve this Policy Senior Management supports the objective put into place by this policy.

1.5 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within OATS, are subject to follow requirements outlined within this policy.

1.6 Compliance

CHFS abides by the security and privacy requirements established in the National Institute of Standards and Technology (NIST), the Internal Revenue Services (IRS), the Social Security Administration (SSA), the Centers for Medicare and Medicaid Services (CMS), as well as other federal and state organizations as the official guidance domain for this policy.

2 Policy Requirements

2.1 General

Commonwealth Office of Technology (COT) staff has limited ability to support users of CHFS network resources that connect from remote sites that are not under the control of COT Field Services staff. This includes users from contract agencies/companies as well as users connecting from home or on the road.

Remote Users will be responsible for a logical progression of troubleshooting.

- Contact their Local Area Network (LAN) technician to determine if their LAN and Wide Area Network (WAN) connection is properly configured and operating appropriately. For home users this would be a combination of their local expert and their Internet Service Provider.
- Contact the Commonwealth Office of Technology (COT) to ensure the remote connection hosts are operational. This includes dial up accounts and Virtual Private Networks (VPN) hosts.
- CHFS technical staff will only be responsible to determine the availability of Cabinet resources once it is determined that a Kentucky Information Highway (KIH) connection exists.

In order to reduce CHFS liability, IT staff will not make or suggest configuration changes to remote non-CHFS equipment or service equipment at personal residence.

CHFS staff is subject to follow all guidelines and requirements as outlined in Enterprise Policy: CIO-076 Firewall and Virtual Private Network Administration Policy.

070.206 CHFS Remote User Support	Current Version: 2.1
070.000 Administrative	Review Date: 01/27/2017

3 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

4 Exceptions

Any exceptions to this policy must follow the procedures established in CHFS OATS IT Policy: 070.203.

5 Policy Review Cycle

This policy is annually reviewed and revised on an as needed basis.

6 References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS IT Policies
- CHFS OATS IT Standards
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- Enterprise IT Policy: CIO-073- Anti-Virus Policy
- Enterprise IT Policy: CIO-076- Firewall and Virtual Private Network Administration Policy
- Internal Revenue Services (IRS) Publications 1075
- National institute of Standards and Technology (NIST) Special Publication 800-18 Guide for Developing Security Plans for Federal Information Systems
- National institute of Standards and Technology (NIST) Special Publication 800-12 An Introduction to Computer Security
- National institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Framework